Filtrage d'URL

Vous pouvez mettre en œuvre le filtrage d’URL à l’aide des règles de contrôle d’accès.

Présentation du filtrage d’URL

Utilisez la fonction de filtrage d’URL pour contrôler les sites Web auxquels les utilisateurs de votre réseau peuvent accéder :

- Filtrage d’URL basé sur la catégorie et la réputation : grâce à une licence de filtrage d’URL, vous pouvez contrôler l’accès aux sites Web en fonction de la classification générale de l’URL (catégorie) et du niveau de risque (réputation). Cette option est recommandée.
- Filtrage manuel d’URL : avec n’importe quelle licence, vous pouvez spécifier manuellement des URL individuelles, des groupes d’URL, des listes d’URL et des flux pour obtenir un contrôle fin et personnalisé sur le trafic Web. Pour en savoir plus, consultez Filtrage manuel des URL, à la page 16.

Consultez également Renseignements de sécurité, une fonctionnalité similaire mais différente permettant de bloquer les URL, les domaines et les adresses IP malveillants.

À propos du filtrage d’URL avec catégorie et réputation

Avec une licence de filtrage d’URL, vous pouvez contrôler l’accès aux sites Web en fonction de la catégorie et de la réputation des URL demandées :

- Catégorie : classification générale pour l'URL. Par exemple, eBay.com appartient à la catégorie Enchères et monster.com appartient à la catégorie Recherche d'emploi.

  Une URL peut appartenir à plusieurs catégories.

- Réputation : la probabilité que l'URL soit utilisée à des fins contraires à la politique de sécurité de votre organisation. Les réputations vont de risque inconnu (niveau 0) ou non fiable (niveau 1) à de confiance (niveau 5).

Avantages du filtrage d'URL basé sur la catégorie et la réputation

Les catégories d'URL et les réputations vous aident à configurer rapidement le filtrage d'URL. Par exemple, vous pouvez utiliser le contrôle d'accès pour bloquer les URL non fiables à dans la catégorie Piratage . Vous pouvez également utiliser la qualité de service QoS pour limiter le trafic des sites de la catégorie en continu. Il existe également des catégories pour les types de menaces, comme la catégorie Logiciel espion et Logiciel publicitaire.

L'utilisation des données de catégorie et de réputation simplifie également la création et l'administration des politiques. Elle vous donne l'assurance que le système contrôle le trafic web comme prévu. Étant donné que Cisco met continuellement à jour ses renseignements sur les menaces avec de nouvelles URL, ainsi que de nouvelles catégories et de nouveaux risques pour les URL existantes, le système utilise des informations actualisées pour filtrer les URL demandées. Des sites qui (par exemple) représentent des menaces pour la sécurité ou qui diffusent du contenu indésirable peuvent apparaître et disparaître plus rapidement que vous ne pouvez mettre à jour et déployer de nouvelles politiques.

Voici quelques exemples de la façon dont le système peut s'adapter :

- Si une règle de contrôle d'accès bloque tous les sites de jeux, à mesure que de nouveaux domaines sont enregistrés et classés comme Jeux, le système peut bloquer ces sites automatiquement. De même, si le débit d'une règle de QoS limite tous les sites de diffusion de vidéo en flux continu, le système peut limiter automatiquement le trafic vers les nouveaux sites de continu.
- Si une règle de contrôle d'accès bloque tous les sites contenant des programmes malveillants et qu'une page d'achat est contaminée par un tel logiciel, le système peut reclasser l'URL de Sites d'achats vers Sites de programmes malveillants et bloquer ce site.
- Si une règle de contrôle d'accès bloque les sites de réseaux sociaux non sécurisés et qu'une personne publie un lien sur sa page de profil qui contient des liens vers des charges utiles malveillantes, le système peut faire passer la réputation de la page de Propices sans danger à non fiable, puis la bloquer.

Limites du filtrage basé sur les catégories dans les règles Ne pas déchiffrer politique de déchiffrement

Vous pouvez éventuellement choisir d'inclure des catégories dans votre Politiques de déchiffrement. Ces catégories, également appelées *filtrage d'URL*, sont mises à jour par les services de renseignement de Cisco Talos. Les mises à jour sont basées sur l'apprentissage automatique et l'analyse humaine en fonction du contenu pouvant être récupéré à partir de la destination du site Web et parfois à partir de ses informations d'hébergement et d'enregistrement. La catégorisation n'est *pas* basée sur le secteur vertical déclaré, l'intention ou la sécurité de l'entreprise.

Remarque Ne confondez pas le filtrage d'URL et la détection d'application, qui repose sur la lecture d'une partie du paquet d'un site Web pour déterminer plus précisément de quoi il s'agit (par exemple, un message Facebook ou Salesforce). Pour en savoir plus, consultez Bonnes pratiques pour la configuration du contrôle des applications.

Pour en savoir plus, consultez Utiliser les catégories dans le filtrage d'URL, à la page 8.

Descriptions des catégories d'URL et de la réputation

Descriptions des catégories

Une description de chaque catégorie d'URL est disponible dans https://www.talosintelligence.com/categories.

Assurez-vous de cliquer sur **Threat Catégories** (Catégories de menaces) pour voir ces catégories.

Descriptions des niveaux de réputation

Allez à https://talosintelligence.com/reputation_center/support et regardez dans la section des questions courantes.

Données de filtrage d'URL de Cisco Cloud (nuage Cisco)

L'ajout d'une licence de filtrage d'URL active automatiquement la fonction de filtrage d'URL. Cela permet le traitement du trafic en fonction de la classification générale, ou de *la catégorie*, du niveau de risque ou de la *réputation* du site Web.

Par défaut, lorsque les utilisateurs naviguent vers une URL dont la catégorie et la réputation ne sont pas dans un cache local des sites Web précédemment consultés, le système la soumet au nuage pour une évaluation des informations sur les menaces et ajoute le résultat au cache.

Vous pouvez également utiliser un ensemble de données d'URL local de catégories et de réputations, ce qui peut accélérer la navigation sur le Web. Lorsque vous activez (ou réactivez) le filtrage d'URL, centre de gestion interroge automatiquement Cisco concernant les données URL et envoie l'ensemble de données aux périphériques gérés. Ensuite, lorsque les utilisateurs naviguent vers une URL, le système vérifie l'ensemble des données locales et le cache pour obtenir des renseignements sur la catégorie et la réputation avant de soumettre l'URL au nuage pour l'évaluation des renseignements sur les menaces. Pour voir vos options d'utilisation de l'ensemble de données local, y compris comment désactiver complètement les recherches dans le nuage individuelles, consultez Options de filtrage d'URL, à la page 11.

Les mises à jour automatiques des données d'URL sont activées par défaut; nous vous recommandons fortement de ne pas les désactiver.

L'ensemble de catégories d'URL peut changer régulièrement. Lorsque vous recevez une notification de changement, passez en revue vos configurations de filtrage d'URL pour vous assurer que le trafic est géré comme prévu. Pour en savoir plus, consultez Si l'ensemble de catégories d'URL change, prendre des mesures, à la page 24.

Bonnes pratiques pour le filtrage d'URL

Gardez à l'esprit les consignes et limites suivantes s'appliquant au filtrage d'URL :

'filtrer par catégorie et réputation

Suivez les instructions qui s'affichent dans Configurer le filtrage d'URL avec catégorie et réputation, à la page 9.

Configurez votre politique pour inspecter les paquets qui doivent être transmis avant qu'une URL ne puisse être identifiée

Le système ne peut pas filtrer les URL avant que :

- Une connexion surveillée soit établie entre un client et le serveur.
- Le système identifie l'application DNS, HTTP ou HTTPS dans la session.
- Le système identifie le domaine ou l'URL demandée (pour les sessions chiffrées, à partir d' un nom de domaine non chiffré, du message ClientHello ou du certificat du serveur).

Cette identification devrait se produire dans les 3 à 5 paquets, ou après l'échange du certificat du serveur dans la prise de contact TLS/SSL si le trafic est chiffré.

Important! Pour vous assurer que votre système examine ces paquets initiaux qui réussiraient à passer autrement, consultez Inspection des paquets qui passent avant que le trafic ne soit identifié et les sous-sections.

Si le trafic précoce correspond à toutes les autres conditions de règle, mais que l'identification est incomplète, le système permet au paquet de passer et l'établissement de la connexion (ou le dialogue de l'établissement de liaison TLS/SSL) . Une fois que le système a terminé son identification, il applique la règle d'action appropriée au trafic de session restant.

Bloquer les catégories de menaces

Assurez-vous que vos politiques traitent spécifiquement des catégories de menaces, qui identifient les sites malveillants connus. Faites cela en plus de bloquer les sites ayant mauvaise réputation.

Par exemple, pour protéger votre réseau contre les sites malveillants, vous devez bloquer toutes les catégories de menace. En outre, Talos recommande de ne bloquer que les sites de la catégorie Médiocre. Vous pouvez bloquer les réputations douteuses si vous avez une posture de sécurité volontariste, mais cela peut entraîner une quantité plus élevée de faux positifs.

Pour en savoir plus, consultez **Catégories de menaces** à l'URL dans Descriptions des catégories d'URL et de la réputation, à la page 3.

Conditions URL et ordre des règles

- Positionnez les règles d'URL après toutes les autres règles à *atteindre*.
- Les URL peuvent appartenir à plusieurs catégories. Il est possible de vouloir autoriser une catégorie de sites Web et d'en bloquer une autre, que ce soit explicitement ou en se fondant sur l'action par défaut. Dans ce cas, assurez-vous de créer et de trier les règles d'URL de manière à obtenir l'effet souhaité, selon que l'autorisation ou le blocage doivent prévaloir.

Pour obtenir des instructions supplémentaires sur les règles, consultez les rubriques suivantes : Bonnes pratiques pour les règles de contrôle d'accès.

URL non catégorisées ou sans réputation

Lorsque vous créez une règle d'URL, vous choisissez d'abord la catégorie à laquelle vous souhaitez la mettre en correspondance. Si vous choisissez explicitement les URL **non catégorisée**, vous ne pouvez pas restreindre davantage selon la réputation.

Les URL non catégorisées avec une réputation non fiable sont gérées par la catégorie **sites malveillants**. Si vous souhaitez bloquer des sites non catégorisés avec tout autre niveau de réputation (comme douteux), vous devez bloquer tous les sites non classés.

Après avoir sélectionné une catégorie et un niveau de réputation, vous pouvez éventuellement sélectionner **Apply to unknown reputation** (Appliquer à une réputation inconnue). Par exemple, vous pouvez créer une règle qui s'applique aux sites ayant une réputation Non fiable, Douteuse ou Inconnue.

Vous ne pouvez pas attribuer manuellement des catégories et des réputations aux URL, mais dans les politiques de contrôle d'accès et de QoS, vous pouvez bloquer manuellement des URL spécifiques. Consultez Filtrage manuel des URL, à la page 16. Consultez aussi Litige relatif aux catégories d'URL et réputations, à la page 23.

Filtrage d'URL pour le trafic Web chiffré

Lors du filtrage d'URL sur le trafic Web chiffré, le système :

- (Si le filtrage DNS est activé) Vérifie si le système a déjà vu le domaine d'origine ou si le domaine est dans la base de données de réputation locale et, si oui, prend des mesures en fonction de la réputation et de la catégorie du domaine. Sinon, le système traite le trafic en fonction de vos configurations pour le trafic chiffré, même si **la nouvelle tentative de recherche dans le cache d'URL** est activée dans les paramètres avancés de la politique de contrôle d'accès.
- Ne tient pas compte du protocole de chiffrement; une règle correspond à la fois au trafic HTTPS et HTTP si la règle a une condition d'URL mais pas une condition d'application qui spécifie le protocole.
- N'utilise pas de listes d'URL. Vous devez plutôt utiliser des objets et des groupes URL.
- Fait correspondre le trafic HTTPS en fonction du nom commun du sujet dans le certificat de clé publique utilisé pour chiffrer le trafic et évalue également la réputation de toute autre URL présentée à tout moment au cours de la transaction, y compris l'URL HTTP post-déchiffrement.
- Ne prend pas en compte les sous-domaines dans le nom commun du sujet.
- N'affiche pas de page de réponse HTTP pour les connexions chiffrées bloquées par les règles de contrôle d'accès (ou toute autre configuration); voir Limites des pages de réponse HTTP, à la page 19.

Filtrage des URL et découverte de l'identité du serveur TLS

La dernière version du protocole TLS (Transport Layer Security) 1.3, définie par la RFC 8446, est le protocole privilégié de nombreux serveurs Web pour fournir des communications sécurisées. Étant donné que le protocole TLS 1.3 chiffre le certificat du serveur pour plus de sécurité, et que le certificat est nécessaire pour correspondre aux critères de filtrage d'application et d'URL dans les règles de contrôle d'accès, le système Firepower permet d'extraire le certificat du serveur *sans* déchiffrer le paquet en entier.

Les paramètres avancés de la politique de contrôle d'accès offrent une option de **détection précoce de l'application et de catégorisation d'URL** pour la découverte de l'identité du serveur TLS.

Nous vous recommandons fortement de l'activer pour tout trafic que vous souhaitez mettre en correspondance avec des critères d'application ou d'URL, en particulier si vous souhaitez effectuer une inspection approfondie de ce trafic. Un politique de déchiffrement n'est pas requis, car *le trafic n'est pas déchiffré* lors du processus d'extraction du certificat de serveur.

Remarque

- Comme le certificat est déchiffré, la découverte d'identité du serveur TLS peut réduire les performances en fonction de la plateforme matérielle.
- La découverte d'identité de serveur TLS n'est pas prise en charge dans les déploiements en mode Tap en ligne ou en mode passif.
- L'activation de la découverte d'identité du serveur TLS n'est prise en charge sur aucun Cisco Secure Firewall Threat Defense Virtual déployé sur AWS. Si de tels périphériques gérés sont gérés par Cisco Secure Firewall Management Center, l'événement de connexion **PROBE_FLOW_DROP_BYPASS_PROXY** est incrémenté chaque fois que le périphérique tente d'extraire le certificat du serveur.

Pour en savoir plus, consultez Paramètres avancés de politique de contrôle d'accès.

HTTP/2

Le système peut extraire les URL HTTP/2 de certificats TLS, mais pas d'une charge utile.

Filtrage manuel des URL

- Spécifier des URL à l'aide d'une liste personnalisée de Security Intelligence ou d'un objet de flux. N'utilisez pas d'objet URL et n'saisissez pas une URL directement dans la règle. Pour de plus amples renseignements, consultez la section Options de filtrage manuel d'URL, à la page 17.
- Si vous filtrez manuellement des URL spécifiques à l'aide d'objets URL ou en entrant des URL directement dans la règle, étudiez attentivement les autres trafics qui pourraient être affectés. Pour déterminer si le trafic réseau correspond à une condition d'URL, le système effectue une simple correspondance de sous-chaîne. Si l'URL demandée correspond à une partie de la chaîne, les URL sont considérées comme correspondantes.
- Si vous utilisez le filtrage d'URL manuel pour créer des exceptions à d'autres règles, placez la règle spécifique avec les exceptions au-dessus de la règle générale qui s'appliquerait sinon.

Rechercher les paramètres de requête dans les URL

Le système n'utilise pas les paramètres de la requête de recherche dans l'URL pour faire correspondre les conditions de l'URL. Par exemple, envisageons un scénario dans lequel vous bloquez tout le trafic d'achat. Dans ce cas, l'utilisation d'une recherche sur le Web pour rechercher amazon.com n'est pas bloquée, mais la navigation sur amazon.com l'est.

Filtrage d'URL dans les déploiements à haute disponibilité

Pour obtenir des consignes sur le filtrage d'URL avec les centres de gestion Firepower Management Center (FMC) en haute disponibilité, consultez *Filtrage d'URL et renseignements sur la sécurité* dans Guide d'administration Cisco Secure Firewall Management Center.

Limites de mémoire pour les modèles de périphériques sélectionnés

- Les modèles de périphériques avec moins de mémoire stockent moins de données URL localement, et le système peut donc vérifier le nuage plus fréquemment pour déterminer la catégorie et la réputation des sites qui ne sont pas dans la base de données locale.

Les périphériques disposant de mémoire plus réduite sont les suivants :

- Firepower 1010
- Défense contre les menaces virtuelles avec 8 Go de RAM

Correspondance d'URL pour la reprise de session TLS sur Threat Defense

Utiliser la mise en correspondance d'URL avec Snort 2 dans les conditions suivantes :

- S'il n'y a pas de reprise de session TLS et que la politique SSL est activée ou que le message Hello de client contient une extension SNI (Server Name Indication).
- Si la reprise de session TLS a lieu et que la politique SSL n'est pas activée ou que le message de client Hello ne contient pas d'extension SNI.

Filtrage du trafic HTTPS

Pour filtrer le trafic chiffré, le système détermine l'URL demandée en fonction des informations transmises lors de la prise de contact TLS/SSL : le nom commun du sujet dans le certificat de clé publique utilisé pour chiffrer le trafic.

Le filtrage HTTPS, contrairement au filtrage HTTP, ne prend pas en compte les sous-domaines du nom commun du sujet. N'incluez pas d'informations de sous-domaine lors du filtrage manuel des URL HTTPS dans les politiques de contrôle d'accès ou de QoS. Par exemple, utilisez exemple.com plutôt que www.exemple.com.

Astuces Dans une Politiques de déchiffrement, vous pouvez gérer et déchiffrer le trafic vers des URL spécifiques en définissant une condition de règle de nom unique politique de déchiffrement. L'attribut de nom commun dans le nom distinctif de sujet d'un certificat contient l'URL du site. Le déchiffrement du trafic HTTPS permet aux règles de contrôle d'accès d'évaluer la session déchiffrée, ce qui améliore le filtrage d'URL.

Contrôle du trafic par le protocole de chiffrement

Le système ne tient pas compte du protocole de chiffrement (HTTP ou HTTPS) lors du filtrage d'URL dans les politiques de contrôle d'accès ou de QoS. Cela se produit pour les conditions d'URL manuelles et basées sur la réputation. Autrement dit, le filtrage d'URL traite le trafic vers les sites Web suivants de manière identique :

- http://example.com/
- par exemple, https://exemple.com

Pour configurer une règle qui correspond uniquement au trafic HTTP ou HTTPS, ajoutez une condition d'application à la règle. Par exemple, vous pourriez autoriser l'accès HTTPS à un site tout en interdisant l'accès HTTP en créant deux règles de contrôle d'accès, chacune comportant une condition d'application et d'URL.

La première règle autorise le trafic HTTPS vers le site Web :

Action : Allow (Autoriser)
Application : HTTPS

URL : example.com

La deuxième règle bloque l'accès HTTP au même site Web :

Action : Bloc (Bloquer)
Application : HTTP
URL : example.com

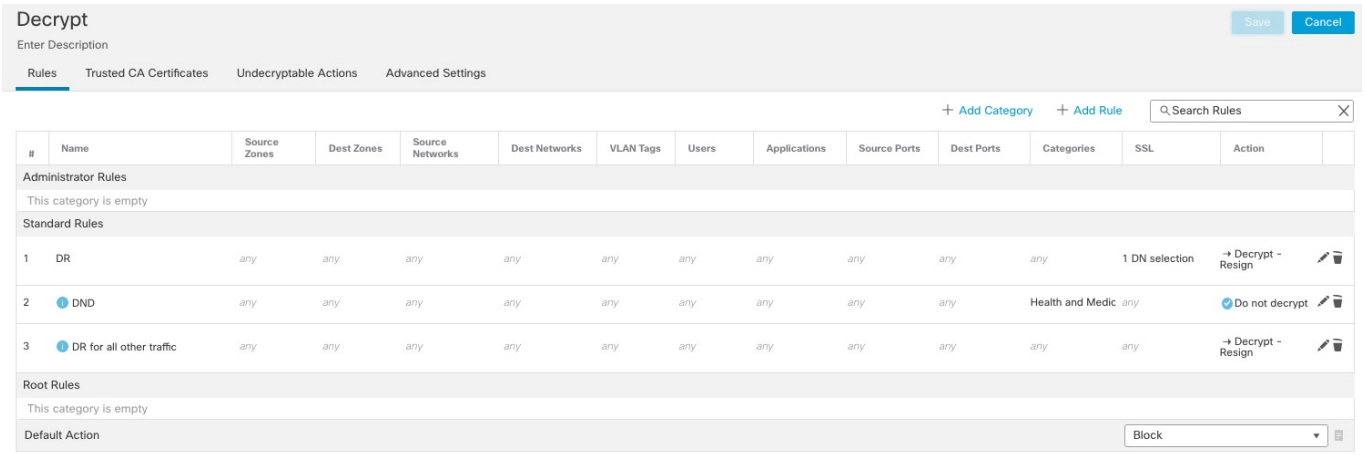
Utiliser les catégories dans le filtrage d'URL

Limites des catégories dans les règles Ne pas déchiffrer

Vous pouvez éventuellement choisir d'inclure des catégories dans votre Politiques de déchiffrement. Ces catégories, également appelées *filtrage d'URL*, sont mises à jour par les services de renseignement de Cisco Talos. Les mises à jour sont basées sur l'apprentissage automatique et l'analyse humaine en fonction du contenu pouvant être récupéré à partir de la destination du site Web et parfois à partir de ses informations d'hébergement et d'enregistrement. La catégorisation n'est *pas* basée sur le secteur vertical déclaré, l'intention ou la sécurité de l'entreprise. Bien que nous nous efforcions de mettre à jour et d'améliorer continuellement les catégories de filtrage d'URL, ce n'est pas une science exacte. Certains sites Web ne sont pas du tout classés et il est possible que certains sites Web soient mal classés.

éviter d'utiliser trop de catégories dans les règles « ne pas déchiffrer » pour éviter le déchiffrement du trafic sans raison; Par exemple, la catégorie Santé et Médecine comprend le site Web WebMD, qui ne menace pas la vie privée des patientes.

Vous trouverez ci-dessous un exemple de politique de déchiffrement qui peut empêcher le déchiffrement des sites Web de la catégorie Santé et Médecine, mais autoriser le déchiffrement pour WebMD et tout le reste. Vous trouverez des renseignements généraux sur les règles de déchiffrement dans Directives pour l'utilisation du déchiffrement TLS/SSL.



Remarque Ne confondez pas le filtrage d'URL et la détection d'application, qui repose sur la lecture d'une partie du paquet d'un site Web pour déterminer plus précisément de quoi il s'agit (par exemple, un message Facebook ou Salesforce). Pour en savoir plus, consultez Bonnes pratiques pour la configuration du contrôle des applications.

Exigences de licence pour le filtrage d'URL

Licence de défense contre les menaces

- Filtrage par catégorie et par réputation : Filtrage d'URL
- Filtrage manuel : aucune licence supplémentaire.

Licence traditionnelle

- Filtrage par catégorie et par réputation : Filtrage d'URL
- Filtrage manuel : aucune licence supplémentaire.

Licences de filtrage d'URL pour les périphériques Threat Defense

Voir les *licences URL* dans le chapitre *Licences* du Guide d'administration de Cisco Secure Firewall Management Center.

Exigences et conditions préalables au filtrage d'URL

Prise en charge des modèles

N'importe lequel

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Configurer le filtrage d'URL avec catégorie et réputation

	Faire ceci	Autres renseignements
Étape 1	Assurez-vous d'avoir les licences adéquates.	Attribuez la licence de filtrage d'URL à chaque périphérique géré qui filtre des URL.

	Faire ceci	Autres renseignements
Étape 2	Assurez-vous que votre centre de gestion peut communiquer avec le nuage pour obtenir des données de filtrage d'URL.	*Exigences d'accès Internet* et *exigences en matière de ports de communication* dans Guide d'administration Cisco Secure Firewall Management Center.
Étape 3	Ayez une bonne compréhension des limites et des lignes directrices, et prenez les mesures nécessaires.	Bonnes pratiques pour le filtrage d'URL, à la page 3
Étape 4	Activez la fonction de filtrage d'URL.	Activer le filtrage d'URL par catégorie et par réputation, à la page 11
Étape 5	Configurez des règles pour filtrer les URL par catégorie et réputation.	Configuration des conditions d'URL, à la page 12 Pour la meilleure protection contre les sites malveillants, vous devez bloquer les sites en fonction de leur réputation ET bloquer les URL dans toutes les catégories de menaces. (Facultatif) Compléter ou remplacer sélectivement le filtrage d'URL basé sur les catégories et la réputation, à la page 18
Étape 6	(Facultatif) Autorisez les utilisateurs à contourner le blocage d'un site Web en cliquant sur dans une page d'avertissement.	Configurer les pages de réponse HTTP, à la page 18
Étape 7	Ordonnez vos règles de sorte que le trafic atteigne les règles clés en premier.	Ordre des règles d'URL
Étape 8	(Facultatif) Modifiez les options avancées liées au filtrage d'URL.	En général, utilisez les valeurs par défaut, sauf si vous avez une raison précise de les modifier. Pour en savoir plus sur les options avancées, notamment les suivantes, consultez Paramètres avancés de politique de contrôle d'accès. • **Nombre maximal de caractères URL à stocker dans les événements de connexion** • **Autoriser un blocage interactif à contourner le blocage pendant (secondes)** • **Réessayer une recherche qui n'a pas réussi dans la cache d'URL** • **Activer l'application de réputation sur le trafic DNS**
Étape 9	Déployez vos modifications.	Déployer les modifications de configuration

	Faire ceci	Autres renseignements
Étape 10	Veillez à ce que votre système reçoive les futures mises à jour de données URL comme prévu	Configurer les moniteurs d'intégrité du filtrage d'URL, à la page 23
Étape 11	Assurez-vous d'avoir activé d'autres fonctionnalités qui protègent votre réseau contre les sites malveillants	Consultez Renseignements de sécurité.

Activer le filtrage d'URL par catégorie et par réputation

Vous devez être un utilisateur administrateur pour effectuer cette tâche.

Avant de commencer

Remplir les conditions préalables décrites en Configurer le filtrage d'URL avec catégorie et réputation, à la page 9.

Procédure

Étape 1 Choisissez **Intégration** > **Autres intégrations**.

Étape 2 Cliquez sur **Services infonuagiques**.

Étape 3 Configurez Options de filtrage d'URL, à la page 11.

Étape 4 Cliquez sur **Save** (enregistrer).

Options de filtrage d'URL

L'ajout d'une licence de filtrage d'URL active automatiquement la fonction de filtrage d'URL. Cela permet le traitement du trafic en fonction de la classification générale, ou de *la catégorie*, du niveau de risque ou de la *réputation* du site Web.

Bien que le système soit configuré par défaut pour soumettre toutes les URL au nuage pour l'évaluation des informations sur les menaces, l'utilisation d'un ensemble de données local de catégories et de réputation peut accélérer la navigation sur le Web. Lorsque vous activez (ou réactivez) le filtrage d'URL, centre de gestion interroge automatiquement Cisco concernant les données URL et envoie l'ensemble de données aux périphériques gérés. Ce processus peut prendre du temps.

Si vous utilisez des règles SSL pour gérer le trafic chiffré, consultez également Lignes directrices et limites relatives à Règle de déchiffrement.

Activer les mises à jour automatique

Si vous **activez les mises à jour automatiques** (valeur par défaut), centre de gestion vérifie le nuage toutes les 30 minutes pour vérifier l'existence de mises à jour. Si vous avez besoin d'un contrôle strict sur le moment où le système contacte les ressources externes, désactivez les mises à jour automatiques et créez plutôt une tâche récurrente à l'aide du planificateur. Consultez *Mises à jour automatisées du filtrage d'URL à l'aide d'une tâche planifiée* du Guide d'administration Cisco Secure Firewall Management Center .

Mettre à jour maintenant

Cliquez sur **Update Now** (Mettre à jour maintenant) pour effectuer une mise à jour unique des données URL à la demande. Vous ne pouvez pas démarrer une mise à jour sur demande si une mise à jour est déjà en cours. Bien que les mises à jour quotidiennes aient tendance à être de taille plus réduite, si plus de cinq jours se sont écoulés depuis votre dernière mise à jour, le téléchargement des nouvelles données URL peut prendre jusqu'à 20 minutes, selon votre bande passante. Ensuite, la mise à jour peut prendre jusqu'à 30 minutes pour effectuer la mise à jour proprement dite.

Source de la requête URL

Vous pouvez choisir la façon dont le système attribue une catégorie et une réputation aux URL que vos utilisateurs consultent. À vous de choisir :

- **Base de données locale uniquement** : utilise l'ensemble de données local uniquement. Utilisez cette option si vous ne souhaitez pas soumettre vos URL non catégorisées (catégorie et réputation hors de l'ensemble de données local) à Cisco, par exemple, pour des raisons de confidentialité. Cependant, notez que les connexions aux URL non catégorisées ne correspondent *pas* aux règles avec des conditions d'URL basées sur la catégorie ou la réputation. Vous ne pouvez pas affecter manuellement des catégories ou des réputations aux URL.
- **Base de données locale et Cisco Cloud** : utilise l'ensemble de données local lorsque cela est possible, ce qui peut accélérer la navigation sur le Web. Lorsque les utilisateurs naviguent vers une URL dont la catégorie et la réputation ne sont pas dans l'ensemble de données local ou dans une mémoire cache de sites Web consultés précédemment, le système la soumet au nuage pour évaluer les menaces et ajoute le résultat à la mémoire cache.
- **Cisco Cloud uniquement** (par défaut) : n'utilise pas l'ensemble de données local. Lorsque les utilisateurs naviguent vers une URL dont la catégorie et la réputation ne sont pas dans un cache local de sites Web consultés précédemment, le système la soumet au nuage pour une évaluation des menaces et ajoute le résultat au cache. Cette option garantit les informations les plus à jour sur la catégorie et la réputation.

  Cette option nécessite Threat Defense version 7.3. Si vous activez cette option, les périphériques exécutant des versions antérieures utiliseront la **base de données locale et l'option Cisco Cloud**.

Les URL mises en mémoire cache expirent

La mise en cache des données de catégorie et de réputation accélère la navigation sur le Web. Par défaut, les données en cache des URL n'expirent jamais, ce qui accélère les performances.

Pour minimiser le nombre de correspondances d'URL sur des données périmées, vous pouvez définir l'expiration des URL dans le cache. Pour une précision et une actualité accrues des données sur les menaces, choisissez un délai d'expiration plus court. Une URL en cache est actualisée *après* la première fois qu'un utilisateur du réseau y accède après le délai spécifié. Le premier utilisateur ne voit pas le résultat actualisé, mais l'utilisateur suivant qui visite cette URL ne voit pas le résultat actualisé.

Configuration des conditions d'URL

Protégez votre réseau en contrôlant l'accès aux sites en fonction de la catégorie d'URL et de la réputation.

Avant de commencer

Attention Comme condition préalable, assurez-vous d'avoir créé au moins une règle Surveiller au sommet des priorités de votre politique de contrôle d'accès, contenant les paramètres de catégorie ou de réputation. Cela est essentiel pour afficher TOUTES les données de catégorie ou de réputation pour TOUTES les URL qui correspondent à la politique de contrôle d'accès concernée.

S'il n'y a aucune règle dans la politique de contrôle d'accès avec les paramètres de catégorie ou de réputation configurés, la page des **événements de connexion** dans le centre de gestion n'affiche aucune donnée pour la catégorie ou la réputation pour tout trafic URL qui atteint la politique de contrôle d'accès.

Procédure

Étape 1 Dans l'éditeur de règles, cliquez sur ce qui suit pour les conditions d'URL :

- Contrôle d'accès ou QoS : Cliquez sur **les URL**.
- SSL : cliquez sur **Catégorie**.

Étape 2 Recherchez et choisissez les catégories d'URL que vous souhaitez contrôler :

Dans une règle de contrôle d'accès ou de QoS, cliquez sur **Catégorie**.

Pour une protection efficace contre les sites malveillants, vous devez bloquer les URL dans toutes les catégories de menace. En outre, Talos recommande de ne bloquer que les sites de la catégorie Médiocre. Vous pouvez bloquer les réputations douteuses si vous avez une posture de sécurité volontariste, mais cela peut entraîner une quantité plus élevée de faux positifs. Pour obtenir la liste des Catégories de menaces, consultez Descriptions des catégories d'URL et de la réputation, à la page 3.

Assurez-vous de cliquer sur les flèches au bas de la liste pour voir toutes les catégories disponibles.

Étape 3 (Facultatif) Limitez les catégories d'URL en choisissant un niveau de **réputation**.

Notez que si vous faites correspondre explicitement des URL **non catégorisées**, vous ne pouvez pas restreindre davantage le trafic par la réputation. Le choix d'un niveau de réputation inclut également d'autres réputations plus ou moins graves que le niveau que vous choisissez, selon l'action de la règle :

- Comprend les réputations moins graves : si la règle autorise ou fait confiance au trafic Web. Par exemple, si vous configurez une règle de contrôle d'accès pour autoriser la catégorie Favorable (niveau 4), elle autorise également automatiquement les sites de Confiance (niveau 5).
- Comprend les réputations plus graves : si la règle de débit limite, déchiffre, bloque ou surveille le trafic Web. Par exemple, si vous configurez une règle de contrôle d'accès pour bloquer les sites Douteux (niveau 2), elle bloque également les sites Non fiables (niveau 1).

Si vous modifiez l'action découlant de la règle, le système modifie automatiquement les niveaux de réputation dans les conditions d'URL.

Vous pouvez également sélectionner **Apply to unknown reputation** (Appliquer à une réputation inconnue).

Étape 4 Cliquez sur **Add URL** (Ajouter une URL) ou **Add to Rule**(ajouter à la règle), ou effectuez un glisser-déposer.

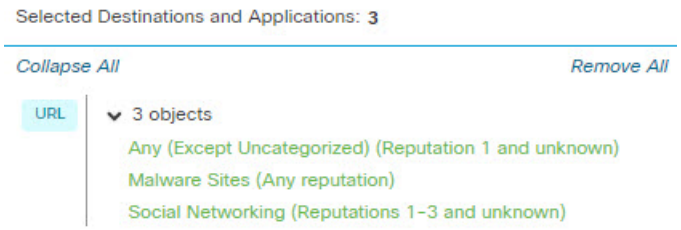
Étape 5 (Facultatif) Pour choisir des objets URL prédéfinis, ou des listes et des flux d'URL dans une règle de contrôle d'accès ou de QoS, cliquez sur **URL**, sélectionnez les objets et ajoutez-les à la destination.

Ces objets mettent en œuvre le filtrage d'URL manuel plutôt qu'un filtrage basé sur la catégorie.

Étape 6 Enregistrez ou continuez à modifier la règle.

Exemple : condition d'URL dans une règle de contrôle d'accès

Le graphique suivant montre la condition d'URL pour une règle de contrôle d'accès qui bloque tous les sites malveillants, tous les sites non fiables et tous les sites de réseaux sociaux avec un niveau de réputation neutre ou inférieur.



Le tableau suivant résume la création de la condition.

URL bloquée	Catégorie	Réputation
Sites de programmes malveillants, quelle que soit leur réputation	Sites de logiciels malveillants	N'importe lequel
Toute URL non fiable (niveau 1)	N'importe lequel	1 – Non fiable
Sites de réseaux sociaux ayant un niveau de réputation neutre ou inférieur (niveaux 1 à 3)	réseau social	3 – Neutre

Règles avec conditions d'URL

Le tableau suivant répertorie les règles qui prennent en charge les conditions d'URL et les types de filtrage pris en charge par chaque type de règle.

Type de règle	Prend en charge le filtrage par catégorie et par réputation?	Prend en charge le filtrage manuel?
Contrôle d'accès	Oui	Oui
Politique de déchiffrement	Oui	Non; utilisez plutôt des conditions de nom distinctif
Qualité de service	Oui	Oui

Pour utiliser le filtrage d'URL dans u de déchiffrement qui a des conditions de règle **Ne pas déchiffrer**, consultez Utiliser les catégories dans le filtrage d'URL, à la page 8.

Ordre des règles d'URL

Pour optimiser la mise en correspondance d'URL, placez des règles qui incluent les conditions d'URL avant les autres règles, en particulier si les règles d'URL sont des règles de blocage et que les autres règles répondent aux deux critères suivants :

- Ils comprennent des conditions d'application.
- Le trafic à inspecter est chiffré.

Si vous configurez des exceptions à une règle, placez l'exception avant l'autre règle.

Filtrage DNS : identifier la réputation et la catégorie d'URL lors de la recherche DNS

L'option **Activer l'application de la réputation sur le trafic DNS** est activée par défaut sous l'onglet **Avancé** de chaque nouvelle politique de contrôle d'accès. Cette option modifie légèrement le comportement du filtrage d'URL et s'applique uniquement lorsque le filtrage d'URL est activé et configuré.

Lorsque cette option est activée :

- Le système évalue la catégorie et la réputation du domaine au début des transactions URL, lorsque le navigateur recherche le nom de domaine pour obtenir l'adresse IP.
- La catégorie et la réputation du trafic chiffré peuvent souvent être déterminées sans déchiffrement

  Si le filtrage DNS ne peut pas déterminer l'URL du trafic chiffré, ce trafic est traité en utilisant vos configurations pour le trafic chiffré.

Activer le filtrage DNS pour identifier les URL lors de la recherche dans le domaine

Le filtrage DNS est activé par défaut dans les nouvelles politiques de contrôle d'accès. Cependant, des configurations supplémentaires peuvent être nécessaires pour que ce paramètre prenne effet.

Avant de commencer

- Le filtrage d'URL à l'aide de la catégorie et de la réputation doit être sous licence, il doit être activé et configuré.

  (Le filtrage DNS n'utilise pas les paramètres suivants dans l'onglet URL : les groupes d'URL, les objets URL, les listes d'URL et les flux, et les URL saisies dans la zone de texte « Enter URL ».)
- Consultez les limites en Limites du filtrage DNS, à la page 16.

Procédure

Étape 1 Dans les paramètres avancés de votre politique de contrôle d'accès, sélectionnez **Enable reputation enforcement on DNS traffic** (Activer la mise en application de la réputation sur le trafic DNS).

Étape 2 Dans la même politique, pour chaque règle de contrôle d'accès pour laquelle une catégorie d'URL et un blocage de la réputation sont configurés :

- Conditions d'application : Si la condition d'application est autre que **toute** (ou vide), ajoutez **DNS** à cette liste. Les autres options liées au DNS ne sont pas pertinentes dans ce contexte.
- Condition de port : Si la condition de port/protocole est autre que **toute** (ou vide), ajoutez **DNS_over_TCP** et **DNS_over_UDP**.

Étape 3 Enregistrez vos modifications.

Prochaine étape

Si vous avez terminé vos modifications : Déployer les modifications de configuration.

Limites du filtrage DNS

Le trafic correspondant aux règles ayant l'action **Block with reset** (blocage avec réinitialisation), **Interactive Block** (blocage interactif) ou **Interactive Block with reset** (blocage interactif avec réinitialisation) sera traité comme si l'action liée à la règle était **Block** (Bloquer).

Les utilisateurs finaux qui tentent d'accéder à une URL bloquée constateront une incapacité inexpliquée à se connecter à leur page; la connexion s'établira puis s'interrompra.

Filtrage DNS et événements

Les événements de connexion générés par le filtrage DNS sont enregistrés à l'aide des champs suivants : requête DNS, Catégorie d'URL, Réputation d'URL et Port de destination. Le champ DNS Query contient le nom de domaine; le champ URL sera vide pour les correspondances de filtrage DNS. Le port de destination sera 53.

De plus:

- Lorsque l'action de la règle de contrôle d'accès est **Allow** (autorisation) ou **Trust**(confiance) , deux événements de connexion sont générés pour le même trafic, un pour le filtrage DNS (avec le champ **DNS Query** rempli) et un pour le filtrage d'URL (avec le champ **URL** rempli).
- La première fois que le système rencontre une URL particulière, vous verrez deux événements pour cette seule session : un événement indiquant « non classé/sans réputation » pour la requête DNS, et un événement indiquant la catégorie et la réputation réelles de l'URL, qui ont été récupérés lors du DNS Requête et appliquées à la session lors du traitement à l'aide du filtrage d'URL standard.

Filtrage manuel des URL

Dans les règles de contrôle d'accès et de QoS, vous pouvez compléter ou remplacer de manière sélective le filtrage d'URL basé sur la catégorie et la réputation en filtrage manuel des URL individuelles, des groupes d'URL ou des listes d'URL et des flux.

Par exemple, vous pourriez utiliser le contrôle d'accès pour bloquer une catégorie de sites Web qui ne conviennent pas à votre organisation. Toutefois, si la catégorie contient un site Web approprié et auquel vous souhaitez fournir l'accès, vous pouvez créer une règle Allow (autorisation) manuelle pour ce site et la placer avant la règle Block (blocage) pour la catégorie concernée.

Vous pouvez effectuer ce type de filtrage d'URL sans licence spéciale.

Le filtrage manuel d'URL n'est pas pris en charge dans les règles SSL; utilisez plutôt des conditions de nom unique.

Mise en garde Selon la façon dont vous mettez en œuvre le filtrage d'URL manuel, la mise en correspondance d'URL peut ne pas être ce que vous souhaitez. Consultez Options de filtrage manuel d'URL, à la page 17.

Options de filtrage manuel d'URL

Il existe plusieurs façons de préciser les URL pour le filtrage d'URL manuel :

Option	Description
(Bonnes pratiques) Utiliser des listes d'URL ou des objets de flux personnalisés de renseignements sur la sécurité.	Il s'agit de la méthode recommandée pour le filtrage manuel d'URL. Vous pouvez créer une liste ou un flux, ou en choisir une existante dans une règle de contrôle d'accès ou de qualité de service. Pour en savoir plus, consultez Listes et flux de renseignements sur la sécurité personnalisés et les sous-sections.
Utiliser des objets URL, individuellement ou en groupe. Les objets URL sont décrits en URL. Ou Saisissez les URL directement dans la règle de contrôle d'accès. (L'option **Enter URL** (Saisir l'URL) sur la page de règle dans l'interface Web.)	Si vous n'incluez pas de chemin (c'est-à-dire qu'il n'y a pas de caractères / dans l'URL), la correspondance est basée sur le nom d'hôte du serveur uniquement. Si vous incluez un ou plusieurs caractères /, la chaîne URL complète est utilisée pour une correspondance de sous-chaîne. Ainsi, une URL est considérée comme en correspondance si l'une des conditions suivantes est remplie : • La chaîne se trouve au début de l'URL. • La chaîne suit un point. • La chaîne contient un point au début. • La chaîne suit les caractères ://. Par exemple, ign.com correspond à ign.com ou www.ign.com, mais pas à versign.com. **Remarque** Nous vous recommandons de ne pas utiliser le filtrage manuel d'URL pour bloquer ou autoriser des pages Web individuelles ou des parties de sites (c'est-à-dire les chaînes URL avec des caractères /), car les serveurs peuvent être réorganisés et les pages déplacées vers de nouveaux chemins. L'option **Enter URL** (Saisir l'URL) ne prend pas en charge les caractères génériques.

Compléter ou remplacer sélectivement le filtrage d'URL basé sur les catégories et la réputation

Dans le contrôle d'accès ou les règles de QoS, vous pouvez utiliser des listes d'URL et de flux Security Intelligence pour compléter ou pour préciser des exceptions à vos règles de filtrage d'URL basées sur la réputation et les catégories.

Important! Si la liste ou le flux que vous configurez dans cette procédure contient des exceptions aux règles basées sur la catégorie ou la réputation, placez cette règle au-dessus de ces règles dans l'ordre des règles.

Dans les règles SSL, utilisez des conditions de nom unique pour configurer le comportement en parallèle.

Avant de commencer

- Configurer le filtrage d'URL par catégorie et réputation. Consultez Configuration des conditions d'URL, à la page 12.
- Comprendre les bonnes pratiques importantes pour le filtrage manuel d'URL. Consultez Bonnes pratiques pour le filtrage d'URL, à la page 3 et Options de filtrage manuel d'URL, à la page 17.
- Configurez un ou plusieurs objets Security Intelligence (listes ou flux) contenant les URL que vous souhaitez utiliser pour le filtrage manuel. Consultez Listes et flux de renseignements sur la sécurité personnalisés.

Procédure

Étape 1 Accédez à la politique de contrôle d'accès ou de QoS dans laquelle vous définirez la règle.

Étape 2 Créez ou modifiez la règle dans laquelle vous ajouterez la nouvelle condition :

- Si vous complétez une règle de filtrage d'URL basée sur la catégorie ou la réputation, modifiez la règle existante.
- Si vous remplacez ou créez des exceptions à une règle de filtrage d'URL basée sur la catégorie ou la réputation, créez une nouvelle règle.

Étape 3 Sélectionnez la liste ou le flux que vous avez créé comme critères d'URL de destination.

Étape 4 Enregistrer la règle

Configurer les pages de réponse HTTP

Dans le cadre du contrôle d'accès, vous pouvez configurer une *page de réponse HTTP* à afficher lorsque le système bloque les requêtes Web, à l'aide des règles de contrôle d'accès ou de l'action par défaut de la politique de contrôle d'accès.

La page de réponse affichée dépend de la façon dont vous bloquez la session :

- **Page de blocage de réponse** : remplace la page par défaut du navigateur ou du serveur qui explique que la connexion a été refusée.

- **Page interactive de réponse de blocage** : met en garde les utilisateurs, mais leur permet également de cliquer sur un bouton (ou d'actualiser la page) pour téléverser le site initialement demandé. Les utilisateurs peuvent avoir à actualiser après avoir contourné la page de réponse pour téléverser les éléments de la page qui ne se sont pas chargés.

Si vous ne choisissez pas une page de réponse, le système bloque les sessions sans interaction ni explication.

Limites des pages de réponse HTTP

Les pages de réponse sont destinées aux règles de contrôle d'accès et aux actions par défaut seulement

Le système affiche une page de réponse uniquement pour les connexions HTTP/HTTPS non chiffrées ou déchiffrées bloquées (ou bloquées de manière interactive) par les règles de contrôle d'accès ou par l'action par défaut de la politique de contrôle d'accès. Le système n'affiche pas de page de réponse pour les connexions bloquées par une autre politique ou un autre mécanisme.

L'affichage de la page de réponse désactive la réinitialisation de la connexion

Le système ne peut pas afficher de page de réponse si la connexion est réinitialisée (paquet RST envoyé). Si vous activez les pages de réponse, le système donne la priorité à cette configuration. Même si vous choisissez **Bloquer avec réinitialisation** ou **Blocage interactif avec réinitialisation** comme action de règle, le système affiche la page de réponse et ne réinitialise pas les connexions Web correspondantes. Pour vous assurer que les connexions Web bloquées sont réinitialisées, vous devez désactiver les pages de réponse.

Notez que tout le trafic non Web qui correspond à la règle *est* bloqué avec une réinitialisation.

Page Pas de réponse pour les connexions chiffrées (doit déchiffrer)

Le système n'affiche pas de page de réponse pour les connexions chiffrées bloquées par les règles de contrôle d'accès (ou toute autre configuration). Les règles de contrôle d'accès évaluent les connexions chiffrées si vous n'avez pas configuré de politique SSL ou si votre politique SSL transmet le trafic chiffré.

Par exemple, le système ne peut pas déchiffrer les sessions HTTP/2 ou SPDY. Si le trafic Web chiffré à l'aide de l'un de ces protocoles atteint l'évaluation de la règle de contrôle d'accès, le système n'affiche pas de page de réponse si la session est bloquée.

Toutefois, le système affiche une page de réponse pour les connexions déchiffrées par la politique SSL, puis bloquées (ou bloquées de manière interactive) par les règles de contrôle d'accès ou par l'action par défaut de la politique de contrôle d'accès. Dans ce cas, le système chiffre la page de réponse et l'envoie à la fin du flux SSL rechiffré.

Aucune page de réponse pour les connexions « promues »

Le système n'affiche pas de page de réponse lorsque le trafic Web est bloqué en raison d'une règle de contrôle d'accès promu (une règle de blocage placée tôt avec uniquement des conditions de réseau simples).

Page Pas de réponse pour certaines connexions redirigées

Si une URL est saisie sans « http » ou « https » , que le navigateur amorce la connexion sur le port 80, que l'utilisateur fait appel à une page de réponse et que la connexion est ensuite redirigée vers le port 443, l'utilisateur ne verra pas de deuxième page de réponse interactive, car la réponse à cette URL est déjà mise en cache.

Page pas de réponse avant l'identification de l'URL

Le système n'affiche pas de page de réponse lorsque le trafic Web est bloqué avant que le système ait identifié l'URL demandée; voir Bonnes pratiques pour le filtrage d'URL, à la page 3.

Exigences et conditions préalables des pages de réponse HTTP

Prise en charge des modèles

N'importe lequel

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Choix des pages de réponse HTTP

L'affichage fiable des pages de réponse HTTP dépend de votre configuration réseau, des charges de trafic et de la taille de la page. Les pages plus petites sont plus susceptibles de s'afficher avec succès.

Procédure

Étape 1 Dans l'éditeur de politique de contrôle d'accès, sélectionnez **Réponses HTTP** à partir de la flèche de la liste déroulante **Plus** à la fin de la ligne de flux de paquets.

Si les contrôles sont grisés, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration. Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.

Étape 2 Choisissez la **page de réponse Block (blocage)** et la **page de réponse Interactive Block (blocage interactif)** :

- Fourni par le système : affiche une réponse générique. Cliquez sur **Afficher** ( ) pour afficher le code de cette page.
- Personnalisé : crée une page de réponse personnalisée. Une fenêtre contextuelle apparaît, préremplie avec le code fourni par le système, que vous pouvez remplacer ou modifier en cliquant sur **Edit** ( ). Un compteur indique le nombre de caractères que vous avez utilisés.
- Aucun : désactive la page de réponse et bloque les sessions sans interaction ni explication. Pour désactiver rapidement le blocage interactif pour l'ensemble de la politique de contrôle d'accès, choisissez cette option.

Étape 3 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Configurer le blocage interactif à l'aide des pages de réponse HTTP

Lorsque vous configurez le blocage interactif, les utilisateurs peuvent téléverser un site demandé à l'origine après avoir lu un avertissement. Les utilisateurs peuvent avoir à actualiser après avoir contourné la page de réponse pour téléverser les éléments de la page qui ne se sont pas chargés.

Astuces Pour désactiver rapidement le blocage interactif pour l'ensemble de la politique de contrôle d'accès, n'affichez ni la page fournie par le système ni une page personnalisée. Le système bloque ensuite toutes les connexions sans interaction.

Si un utilisateur ne contourne pas un blocage interactif, le trafic correspondant est refusé sans autre inspection. Si un utilisateur contourne un blocage interactif, la règle de contrôle d'accès autorise le trafic, bien que le trafic puisse toujours être soumis à une inspection approfondie et à un blocage.

Par défaut, un contournement d'utilisateur est en vigueur pendant 10 minutes (600 secondes) sans que la page d'avertissement ne soit affichée lors des visites suivantes. Vous pouvez définir une durée pouvant atteindre un an, ou vous pouvez forcer l'utilisateur à contourner le blocage à chaque fois. Cette limite s'applique à chaque règle Blocage interactif de la politique. Vous ne pouvez pas définir la limite par règle.

Les options de journalisation pour le trafic bloqué interactivement sont identiques à celles du trafic autorisé, mais si un utilisateur ne contourne pas le blocage interactif, le système ne peut consigner que les événements de début de connexion. Lorsque le système envoie un avertissement initial à l'utilisateur, il marque tout événement de début de connexion d'une action `blocage interactif` ou `blocage interactif avec réinitialisation`. Si l'utilisateur contourne le blocage, les événements de connexion supplémentaires enregistrés pour la session ont une action `Allow`(autorisation) .

Configuration du blocage interactif

La procédure suivante explique comment permettre aux utilisateurs de contourner les règles de filtrage d'URL.

Procédure

Étape 1 Dans le cadre du contrôle d'accès, configurer une règle de contrôle d'accès qui correspond au trafic Web; voir Créer et modifier les règles de contrôle d'accès :

- Action : définissez l'action de la règle sur **Interactive Block** (blocage interactif) ou **Interactive Block with reset** (Blocage interactif avec réinitialisation); voir Actions de blocage interactif des règles de contrôle d'accès.
- Conditions : utilisez des conditions d'URL pour préciser le trafic Web à bloquer de manière interactive; voir Conditions d'URL (filtrage d'URL).
- Journalisation : on suppose que les utilisateurs contourneront le blocage et choisiront les options de journalisation en conséquence.
- Inspection : on suppose que les utilisateurs contourneront le blocage et choisiront les options d'inspection approfondie en conséquence; voir Aperçu du contrôle d'accès.

Étape 2 (Facultatif) Dans la politique de contrôle d'accès **HTTP Responses** (Réponses HTTP), choisissez une page de réponse HTTP personnalisée à blocage interactif; voir Choix des pages de réponse HTTP, à la page 20.

Étape 3 (Facultatif) Dans les paramètres **avancés** de la politique de contrôle d'accès, modifiez le délai d'expiration de contournement de l'utilisateur. voir Définition du délai de contournement d'utilisateur pour un site Web bloqué, à la page 22.

Une fois qu'un utilisateur a contourné un blocage, le système permet à celui-ce d'accéder à cette page sans avertissement jusqu'à ce que le délai d'expiration se soit écoulé.

Étape 4 Enregistrez la politique de contrôle d'accès.

Étape 5 Déployer les changements de configuration.

Définition du délai de contournement d'utilisateur pour un site Web bloqué

La procédure suivante explique comment définir le temps de navigation autorisé après que l'utilisateur ait contourné un blocage de filtrage d'URL. À l'expiration du délai, l'utilisateur doit à nouveau contourner le blocage.

Procédure

Étape 1 Cliquez sur **Politiques** > **Contrôle d'accès** et modifiez la politique.

Étape 2 Sélectionnez **Advanced Settings** (paramètres avancés) depuis la flèche de la liste déroulante **More** (Autres) à la fin de la ligne de flux de paquets.

Étape 3 Cliquez sur **Edit** (✎) à côté de Paramètres généraux.

Si **Afficher** (👁) apparaît au contraire, les paramètres sont hérités d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration. Si la configuration est déverrouillée, décochez la case **Inherit from base policy** (hériter de la politique de base) pour activer la modification.

Étape 4 Dans le champ **Allow an Interactive Block to Bypass Blocking for (seconds)** (autoriser un blocage interactif pendant (secondes)), saisissez le nombre de secondes qui doivent s'exécuter avant l'expiration du contournement de l'utilisateur.

En définissant cette valeur à 0, la réponse du bloc interactif est affichée une seule fois et le contournement de l'utilisateur n'expire jamais.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique.

Prochaine étape

- Déployer les changements de configuration.

Configurer les moniteurs d'intégrité du filtrage d'URL

Les politiques d'intégrité suivantes envoient des alertes si le système éprouve des difficultés à obtenir ou à mettre à jour les données de catégorie d'URL et de réputation.

- Moniteur de filtrage URL
- Mises à jour des périphériques à propos des données sur les menaces

Pour vous assurer qu'ils sont configurés comme vous le souhaitez, consultez *Modules d'intégrité* et *Configuration de la surveillance de l'intégrité* dans Guide d'administration Cisco Secure Firewall Management Center.

Litige relatif aux catégories d'URL et réputations

Si vous êtes en désaccord avec une catégorie ou une réputation attribuée par Talos, vous pouvez soumettre une demande de réévaluation.

Avant de commencer

Vous aurez besoin des identifiants de votre compte Cisco.

Procédure

Étape 1 Dans l'interface Web centre de gestion, effectuez l'une des opérations suivantes :

Option du lieu de la contestation	Option de chemin d'accès à la contestation
Problème de configuration des services en nuage	a. Accédez à la page **Integration** > **Autres intégrations** > **Services en nuage**. b. Sélectionnez **Litige de catégories d'URL et réputations**.
Page de recherche manuelle d'URL	a. Rendez-vous sur la page de recherche manuelle d'URL : **Analyse > Avancé > URL**. b. Recherchez l'URL en question. c. Pour voir la **contestation** à la fin de la ligne du tableau, passez le curseur sur l'entrée pertinente dans la liste des résultats, puis cliquez sur Contester.
Événement de connexion d'URL	a. Dans le menu **Analysis > Connections**, accédez à n'importe quelle page dont le tableau comprend les URL. b. Faites un clic droit sur un élément de la colonne **Catégorie d'URL** ou **Réputation d'URL** (afficher les colonnes masquées si nécessaire) et sélectionnez une option.

Le site Web Talos s'ouvre dans une fenêtre de navigateur distincte.

Étape 2 Connectez-vous au site Talos avec vos informations d'authentification Cisco.

Étape 3 Passez en revue les informations et suivez les instructions sur la page Talos.

Étape 4 Recherchez des informations sur le site Talos sur la façon dont les litiges soumis sont traités et sur la réponse à attendre, le cas échéant.

Le processus de contestation est indépendant des produits Firepower.

Si l'ensemble de catégories d'URL change, prendre des mesures

L'ensemble de catégories de filtrage d'URL peut changer à l'occasion afin de s'adapter aux nouvelles tendances du Web et aux modèles d'utilisation en pleine évolution.

Ces modifications affectent à la fois les politiques et les événements.

Peu de temps avant et après la planification des modifications de catégories d'URL, et après, vous verrez des alertes dans la liste de règles des politiques de contrôle d'accès, de SSL et de QoS touchées par les modifications, et pour les URL ou la catégorie des règles que vous (modifier).

Vous devez agir lorsque vous voyez ces alertes.

Remarque Les mises à jour de l'ensemble de catégories d'URL décrites dans cette rubrique sont distinctes des modifications qui ajoutent simplement de nouvelles URL aux catégories existantes ou reclassent des URL mal classées. Cette rubrique ne s'applique pas aux changements de catégorie pour les URL individuelles.

Procédure

Étape 1 Si vous voyez une alerte à côté d'une règle dans une politique de contrôle d'accès, passez le curseur sur l'alerte pour voir les détails.

Étape 2 Si l'alerte mentionne des modifications apportées aux catégories d'URL, modifiez la règle pour afficher plus de détails.

Étape 3 Passez le curseur sur l'URL ou la catégorie dans la boîte de dialogue de règle pour afficher des informations générales sur le type de modifications.

Étape 4 Si vous voyez une alerte à côté d'une catégorie, cliquez sur l'alerte pour en afficher les détails.

Étape 5 Si vous voyez un lien « Plus d'informations » dans la description d'une modification, cliquez dessus pour afficher les informations sur la catégorie sur le site Web de Talos.

Sinon, consultez une liste et des descriptions de toutes les catégories au lien dans Descriptions des catégories d'URL et de la réputation, à la page 3.

Étape 6 Selon le type de modification, prenez les mesures appropriées :

Type de changement de catégorie	Que fera le système?	Ce que vous devez faire
La catégorie existante sera bientôt obsolète	Rien pour l'instant. Vous avez quelques semaines pour les modifier. Si vous ne prenez aucune mesure pendant ce délai, le système ne pourra pas redéployer la politique.	Supprimez cette catégorie de toutes les règles qui l'incluent. S'il existe une nouvelle catégorie similaire, vous pouvez envisager de l'utiliser plutôt.
Une nouvelle catégorie est ajoutée.	Par défaut, le système n'utilise pas les catégories nouvellement ajoutées.	Vous pouvez créer de nouvelles règles pour la nouvelle catégorie.
La catégorie existante est supprimée	La catégorie s'affichera dans la règle en texte barré (c'est-à-dire avec une ligne dans le nom de la catégorie).	Vous devez supprimer la catégorie obsolète de la règle avant de pouvoir déployer la politique.

Étape 7 Vérifiez vos règles SSL (Catégorie) pour ces modifications et prenez les mesures nécessaires.

Étape 8 Vérifiez vos règles QoS (URL) pour voir ces modifications et prendre les mesures nécessaires.

Prochaine étape

Déployer les changements de configuration.

Changements de catégorie d'URL et de réputation : effet sur les événements

- Lorsque les catégories d'URL changent, les événements traités par le système avant le changement de catégorie sont associés au nom de leur catégorie d'origine et sont étiquetés à l'aide de **Legacy** (Hérité). Les événements traités par le système après le changement de catégorie seront associés aux nouvelles catégories.

  Les événements existants et plus anciens vont disparaître du système avec le temps.

- Si une URL n'a pas de réputation au moment où elle a été traitée, la colonne Réputation d'URL dans la visualisation d'événements sera vide.

Dépannage du filtrage d'URL

La catégorie d'URL attendue est manquante dans la liste des catégories

La fonction de filtrage des URL utilise un ensemble de catégories différent de celui de la fonction de renseignement sur la sécurité (Security Intelligence); la catégorie que vous vous attendez à voir peut être une catégorie de renseignement sur la sécurité. Pour voir ces catégories, consultez l'onglet **URL** de l'onglet **Security Intelligence** dans une politique de contrôle d'accès.

Les paquets initiaux passent non inspectés

Consultez Inspection des paquets qui passent avant que le trafic ne soit identifié et les sous-sections.

Consultez aussi Filtrage DNS : identifier la réputation et la catégorie d'URL lors de la recherche DNS , à la page 15.

Alerte d'intégrité : « URL Filtering registration failure (Échec de l'enregistrement du filtrage d'URL) »

Vérifiez que votre centre de gestion et tous les serveurs mandataires peuvent se connecter au nuage Cisco. Vous pourriez avoir besoin d'informations sur le filtrage d'URL et les catégories d'URL dans les rubriques suivantes : *Exigences d'accès Internet* et *Exigences relatives aux ports de communication* dans les Guide d'administration Cisco Secure Firewall Management Center.

Comment puis-je trouver la catégorie et la réputation d'une URL en particulier?

Effectuez une recherche manuelle. Voir *Recherche de la catégorie et de la réputation d'URL* dans le Guide d'administration Cisco Secure Firewall Management Center.

Erreur lors d'une tentative de recherche manuelle : «Cloud Lookup Failure for<URL>

Assurez-vous que la fonction est correctement activée. Consultez les conditions préalables dans *FRecherche de la catégorie et de la réputation de l'URL* dans le Guide d'administration Cisco Secure Firewall Management Center.

L'URL semble être mal gérée en fonction de sa catégorie et de sa réputation

Problème : le système ne gère pas correctement l'URL en fonction de sa catégorie et de sa réputation.

Solutions :

- Vérifiez que la catégorie et la réputation associées à l'URL correspondent à ce que vous estimez être. Voir *Recherche de la catégorie et de la réputation d'URL* dans le Guide d'administration Cisco Secure Firewall Management Center.
- Les problèmes suivants peuvent être résolus par les paramètres décrits dans Options de filtrage d'URL, à la page 11, accessible en utilisant Activer le filtrage d'URL par catégorie et par réputation, à la page 11.
  - Le cache d'URL peut contenir des informations périmées. Consultez les renseignements sur le paramètre **Expiration des URL en cache** dans Options de filtrage d'URL, à la page 11.
  - L'ensemble de données local peut ne pas être mis à jour avec les informations à jour du nuage. Consultez les informations sur le paramètre **Activer les mises à jour automatiques** dans Options de filtrage d'URL, à la page 11.
  - Le système peut être configuré pour *ne pas* vérifier les données actuelles dans le nuage. Consultez les renseignements sur le paramètre **Rechercher les URL inconnues dans le nuage Cisco** dans Options de filtrage d'URL, à la page 11.
- Votre politique de contrôle d'accès peut être configurée pour transférer le trafic vers l'URL sans vérifier le nuage. Consultez les informations sur le paramètre de **Réessayer la recherche de l'URL manquée dans le cache** dans Paramètres avancés de politique de contrôle d'accès.
- Consultez aussi Bonnes pratiques pour le filtrage d'URL, à la page 3.
- Si l'URL est traitée à l'aide d'une règle SSL, consultez Lignes directrices et limites relatives à Règle de déchiffrement et Ordre des règles SSL

- Vérifiez que l'URL est traitée à l'aide de la règle de contrôle d'accès par laquelle vous pensez qu'elle est traitée, et que la règle fait ce que vous pensez qu'elle fait. Tenez compte de l'ordre des règles.
- Vérifiez que la catégorie d'URL locale et la base de données de réputation sur centre de gestion sont mises à jour avec succès à partir du nuage et que les périphériques gérés sont mis à jour avec succès à partir de centre de gestion.

  L'état de ces processus est signalé dans le moniteur d'intégrité, dans le module du **moniteur de filtrage d'URL** et dans le module **de mise à jour des données de menaces sur les périphériques**. Pour en savoir plus, consultez le chapitre *Intégrité* dans le Guide d'administration Cisco Secure Firewall Management Center .

Si vous souhaitez mettre immédiatement à jour la catégorie d'URL locale et la base de données de réputation, accédez à **Intégration** > **Autres intégrations**, cliquez sur **Services infonuagiques**, puis sur **Update Now** (Mettre à jour maintenant). Pour en savoir plus, consultez Options de filtrage d'URL, à la page 11.

Une catégorie d'URL ou une réputation est incorrecte

Pour les règles de contrôle d'accès ou de qualité de service : utilisez le filtrage manuel en faisant très attention à l'ordre des règles. Consultez Filtrage manuel des URL, à la page 16 et Configuration des conditions d'URL, à la page 12.

Pour les règles SSL : le filtrage manuel n'est pas pris en charge. Utilisez plutôt des conditions de nom unique.

Voir aussi Litige relatif aux catégories d'URL et réputations, à la page 23.

Les pages Web sont lentes à téléverser

Un compromis est réalisé entre sécurité et les performances. Quelques options :

- Envisagez de modifier le **paramètre d'expiration des URL en cache**. Cliquez sur **Intégration** > **Autres intégrations**, puis sélectionnez **Services infonuagiques**. Pour en savoir plus, consultez Options de filtrage d'URL, à la page 11.
- Envisagez de désélectionner le paramètre **Retry URL cache miss lookup**(Retenter la recherche en cas d'échec du cache de l'URL) dans Paramètres avancés de politique de contrôle d'accès.

Les événements n'incluent pas la catégorie d'URL et la réputation

- Vérifiez que vous avez inclus les règles d'URL applicables dans une politique de contrôle d'accès, que les règles sont actives et que les politiques ont été déployées sur les périphériques pertinents.
- La catégorie et la réputation de l'URL ne s'affichent pas dans un événement si la connexion est traitée avant qu'elle ne corresponde à une règle d'URL.
- La règle qui gère la connexion doit être configurée pour la catégorie d'URL et la réputation.
- Même si vous avez configuré des catégories d'URL dans l'onglet Catégories d'une règle SSL, vous devez également configurer l'onglet URL dans une règle de votre politique de contrôle d'accès.

Le filtrage DNS ne fonctionne pas

Assurez-vous d'avoir satisfait à toutes les conditions préalables et à toutes les étapes décrites dans Activer le filtrage DNS pour identifier les URL lors de la recherche dans le domaine , à la page 15.

Un utilisateur final tente d'accéder à une URL bloquée, mais la page ne fait que tourner et expirer

Lorsque le filtrage DNS est activé et que les utilisateurs finaux accèdent à une URL bloquée, la page tourne mais ne se charge pas. Les utilisateurs finaux ne sont pas informés du blocage de la page. Il s'agit actuellement d'une limitation lorsque le filtrage DNS est activé.

Consultez Limites du filtrage DNS, à la page 16.

Les événements incluent la catégorie d'URL et la réputation, mais le champ URL est vide

Si le champ de requête DNS est rempli et que le champ URL est vide, cela est normal lorsque la fonction de filtrage DNS est activée.

Consultez Filtrage DNS et événements, à la page 16.

Plusieurs événements sont générés pour une seule transaction

Une seule transaction Web génère parfois deux événements de connexion, un pour le filtrage DNS et l'autre pour le filtrage d'URL. Cela est attendu lorsque le filtrage DNS est activé et :

- l'action de la règle de contrôle d'accès pour le trafic est Allow (autorisation) ou Trust (confiance).
- le système rencontre une URL pour la première fois.

Consultez Filtrage DNS et événements, à la page 16.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.